Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

Mark S. Reich (*pro hac vice* forthcoming)
Courtney E. Maccarone (*pro hac vice* forthcoming)
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
4th Floor, Suite #427
New York, NY 10006
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: cmaccarone@zlk.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

VANESSA WILLIAMS, ROZALYNN FISHER, LAURA DAY, SARUNY BIN, AND MARLENE CALZADOPAEZ, individually and on behalf of all other similarly situated, Plaintiff, v. **CAESARS ENTERTAINMENT, INC.**, Defendant.	**Case No.** 2:23-cv-1919 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs, ("Plaintiffs") Vanessa Williams, Rozalynn Fisher, Laura Day, Saruny Bin, and Marlene Calzadopaez, individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this Class Action Complaint against Defendant Caesars Entertainment, Inc., ("Defendant" or "Caesars"). Plaintiffs allege the following upon information

and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiffs and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Caesars with sensitive personally identifiable information that was subsequently exposed in a data breach, which Caesars publicly disclosed on or around September 7, 2023 (the "Data Breach" or the "Breach").

2. Plaintiffs' claims arise from Caesars failure to properly secure and safeguard personally identifying information ("PII") [1] that was entrusted to it, and its accompanying responsibility to store and transfer that information. Although, Caesars has not disclosed the exact number of individuals impacted by the Data Breach, it has confirmed that the cybercriminals were able to obtain a copy of Caesar's loyalty program database, including the driver's license numbers and Social Security numbers for a "significant number" of its more than 65 million program members.[2]

3. Caesars is a hospitality and entertainment company that operates destination resorts throughout the United States. Customers who utilize Caesars' service or stay at its resorts may join its "Caesars Rewards" loyalty program, which allows customers to earn points by spending money at Caesars' locations and redeem them for various benefits including complimentary hotel stays, dinners, and casino credits, among other rewards.[3]

4. As a condition of joining Caesars loyalty program, Caesars requires that its customers entrust it with highly sensitive PII. Caesars retains and stores this PII for use in tracking

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] See Zack Whittaker, *Caesars Entertainment says customer data stolen in cyberattack*, TECHCRUNCH (Sept. 14, 2023) https://techcrunch.com/2023/09/14/caesars-entertainment-data-breach-cyberattack/ (last visited November 15, 2023).

[3] See *Caesars Rewards*, CAESARS https://www.caesars.com/myrewards/benefits-overview (last visited November 15, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

loyalty member program points, among other purposes. By obtaining, collecting, and deriving a benefit from its customers' PII, Caesars assumed legal and equitable duties to take reasonable measures to protect their PII. Caesars failed to do so, despite the known risk of theft by cyber criminals.

5. Caesars, on or around September 7, 2023, learned that one of its IT support vendors was the target of a successful cyberattack.[4] In response, Defendant "launched an investigation, engaged leading cybersecurity firms to assist, and notified law enforcement and state gaming regulators."[5] As a result of its investigation, Defendant concluded that an unauthorized actor acquired, among other data, a copy of Defendant's loyalty program database, "which includes driver's license numbers and/or social security numbers for a significant number of members in the database."[6] Tens of millions of customers may have been affected by the Data Breach.[7]

6. Caesars, on September 14, 2023, acknowledged that hackers accessed its computer system that it uses to store sensitive personal information for its customers.[8] Plaintiffs' claims arise from Caesars' failure to safeguard personally identifying information provided by and belonging to its customers, including (without limitation) their name, date of birth, passport number, driver's license number, geolocation data, purchase information, gaming activity information, government identification card number, tax identification number, Social Security number and/or financial account information, and other information such as phone number, address, and email address.

7. Caesars failed to take precautions designed to keep their customers PII secure.

---

[4] *Caesars Informational Website: Learn More*, IDX, A ZEROFOX COMPANY https://response.idx.us/caesars/#learn-more (last visited November 15, 2023).
[5] *Id.*
[6] *Id.*
[7] See Ken Ritter and The Associated Press, *Casino giant Caesars Entertainment hit by cyberattack, joining rival MGM Resorts as victim of data breach*, FORTUNE (Sept. 15, 2023) https://fortune.com/2023/09/15/caesars-entertainment-cyberattack-mgm-resorts-data-breach/ (last visited November 15, 2023).
[8] *Caesars Informational Website: Learn More*, IDX, A ZEROFOX COMPANY https://response.idx.us/caesars/#learn-more (last visited November 15, 2023); see also *SEC Form 8-K, Caesars Entertainment, Inc.*, CAESARS (Sept. 7, 2023) https://investor.caesars.com/static-files/0bc13ee5-34a9-402e-8e7a-824b9dba4e57 (last visited November 15, 2023) .

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

8. Caesars owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the PII Caesars collected safe and secure from unauthorized access. Caesars solicited, collected, used, and derived a benefit from the PII, yet breached its duty by failing to implement or maintain adequate security practices.

9. Ceasars admits that information in its system was accessed by unauthorized individuals.

10. The sensitive nature of the data exposed through the Data Breach, including Social Security numbers, signifies that Plaintiff and Class members have suffered irreparable harm. Plaintiff and Class members have lost the ability to control their private information and are subject to an increased risk of identity theft.

11. Caesars also inexcusably delayed disclosing and providing notice of the Data Breach to its customers. Caesars believes that the Data Breach occurred on August 23, 2023, based on its disclosure to Maine's Attorney General's office on October 6, 2023. However, Caesars first informed the public of the Data Breach in an 8-K Filing with the Securities and Exchange Commission ("SEC") on September 14, 2023—stating that the digital break-in was discovered on September 7, 2023.

12. Caesars failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and members of the Class, causing the exposure of PII for Plaintiff and members of the Class.

13. As a multi-billion-dollar publicly traded company, Caesars had the financial wherewithal and personnel necessary to prevent the Data Breach. Yet, Caesars nevertheless failed to adopt adequate data security measures to prevent such a Data Breach.

14. As a result of the Ceasars' inadequate digital security and notice process, Plaintiff and Class members' PII was exposed to criminals. Plaintiff and the Class have suffered and will continue to suffer injuries including: financial losses caused by misuse of PII; the loss or diminished value of their PII as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

15. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and members of the Class; (ii) warn Plaintiff and members of the Class of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected PII using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and members of the Class of the Data Breach. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

16. Plaintiffs bring this action individually and on behalf of a Nationwide Class and New York, New Jersey, Maryland, and California Subclasses, of similarly situated individuals against Defendant for: negligence; breach of implied contract; violation of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1; violation of the California Consumer Privacy Act ("CPPA"), Cal. Civ. Code § 1798.100, *et. seq*; violation of the California Unfair Competition Act ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*.; violation of the Maryland Consumer Protection Act, MD Code Commercial Law, § 13-301 *et seq*.; violation of the New York General Business Law, N.Y. Gen. Bus. Law §§ 349, *et seq*.; and unjust enrichment.

17. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class members.

19. This Court has personal jurisdiction over Defendant because Defendant maintains their principal place of business in this District. Ceasars's Terms state that "the parties agree that any litigation between them shall be filed exclusively in state or federal courts located in Las Vegas,

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

Nevada (except for small claims court actions which may be brought in the county where you reside). The parties expressly consent to exclusive jurisdiction in Nevada for any litigation other than small claims court actions. "[9]

20. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

PARTIES

21. Plaintiff Vanessa Williams is a citizen of New Jersey and resides in New Brunswick, New Jersey. Ms. Williams received a notice of data breach letter – dated October 13, 2023 – from Caesars informing her that PII was compromised in the Data Breach. As a consequence of the Data Breach, Ms. Williams has been forced to and will continue to invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Since the Data Breach, Ms. Williams was notified that her information was found on the dark web and has noticed an increase in spam calls. Ms. Williams has further had to cancel at least a debit card and a credit card since the Data Breach. Ms. Williams is subject to substantial and imminent risk of future harm.

22. Plaintiff Rozalynn Fisher is a citizen of California and resides in Fontana, California. Ms. Fisher received a notice of data breach letter – dated October 18, 2023 – from Caesars informing her that PII was compromised in the Data Breach. As a consequence of the Data Breach, Ms. Fischer has been forced to and will continue to invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Ms. Fischer has also had to replace her debit card and close her checking account with Navy Federal Credit Union since the Data Breach as she experienced unauthorized charges to her account. Since the Data Breach, Ms. Fisher has also experienced unauthorized login attempts on her Facebook account that uses the same email address as her Navy Federal account. Ms. Fischer is subject to substantial and imminent risk of future harm.

[9] *Terms of Service*, CAESARS https://www.caesars.com/corporate/terms-of-service (last visited November 15, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

23. Plaintiff Laura Day is a citizen of Maryland and resides in Pasadena, Maryland. Ms. Day received a notice of data breach letter – dated October 16, 2023 – from Caesars informing her that PII was compromised in the Data Breach. As a consequence of the Data Breach, Ms. Day has been forced to and will continue to invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Ms. Day is subject to substantial and imminent risk of future harm.

24. Plaintiff Saruny Bin is a citizen of California and resides in Stockton, California. Mr. Bin received a notice of data breach letter – dated October 20,, 2023 – from Caesars informing him that her PII was compromised in the Data Breach. As a consequence of the Data Breach, Ms. Bin has been forced to and will continue to invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Since the Data Breach Ms. Bin has had her Bank of America account compromised, has had to get a new card, change her security questions, password and email associated with her Bank of America Account. Ms. Bin is subject to substantial and imminent risk of future harm.

25. Plaintiff Marlene Calzadopaez is a citizen of New York and resides in Rochester, New York. Ms. Calzadopaez received a notice of data breach letter – dated October 19, 2023 – from Caesars informing him that her PII was compromised in the Data Breach. As a consequence of the Data Breach, Ms. Calzadopaez has been forced to and will continue to invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Further, Ms. Calzadopaez has placed a freeze on her credit due to fear of identity theft, and has noticed an increase in spam emails and calls since the Data Breach. Ms. Calzadopaez is subject to substantial and imminent risk of future harm.

26. Defendant Caesar's Entertainment Inc. is a Delaware corporation that owns and operates entertainment and hospitality establishments throughout the United States. Defendant maintains its principal place of business at 100 West Liberty Street, 12th Floor, Reno, Nevada 89501. Defendant's registered agent for service of process is the Corporation Service Company, located at 2710 Gateway Oaks Drive, Suite 150N, Sacramento, CA 95833-3505.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

FACTUAL BACKGROUND

A. Background on Caesars

21. Defendant is a hospitality and entertainment company that operates destination resorts throughout the United States. Customers who utilize Caesars' service or stay at its resorts may join its "Caesars Rewards" loyalty program, which allows customers to earn points by spending money at Caesars' locations and redeem them for various benefits including complimentary hotel stays, dinners, and casino credits, among other rewards.[10] Caesars Rewards is the largest loyalty program in the gaming industry, with over 60 million members.[11]

22. Plaintiff and Class members are current and former Caesars Rewards members.

23. As a condition of receiving its products and/or services, Defendant requires that its Caesars Rewards members, including Plaintiff and Class members, entrust it with highly sensitive — including, *inter alia*, their names and driver's license numbers and/or social security numbers. Defendant then collects, aggregates, and stores that PII in its internal data servers.

24. Defendant's Privacy Policy provides that it is "committed to respecting your data privacy," and that it "maintain[s] physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control."[12]

25. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class members, that the PII collected from them as a condition of obtaining membership in the Caesars Rewards program would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

26. Plaintiff and Class members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to

---

[10] *Caesars Rewards*, CAESARS https://www.caesars.com/myrewards/benefits-overview (last visited November 15, 2023).
[11] *Id.*
[12] *U.S. Privacy Policy*, CAESARS https://www.caesars.com/corporate/privacy (last visited November 15, 2023).

keep such information confidential and secure from unauthorized access.

27. As a result of collecting and storing the PII of Plaintiff and members of the Class for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Member's PII from disclosure to third parties.

B. The Data Breach

28. On or around August 23, 2023, Caesars had their internal data servers breached by unauthorized third-party hackers, which compromised highly sensitive PII of its loyalty program members - including, *inter alia*, their names, driver's license numbers and social security numbers. The group responsible for the hack is believed to be a hacker group referred to as The Scattered Spider.[13] As a result of their attack, the hackers acquired approximately six terabytes of data from Caesars, which included the PII of its customers.[14]

29. On or about September 7, 2023, Defendant filed a Form 8-K with the SEC in which Caesars disclosed that it had been the target of a cyberattack that led to a data breach.[15] The report asserted:

> Caesars Entertainment, Inc. (the "Company," "we," or "our") recently identified suspicious activity in its information technology network resulting from a social engineering attack on an outsourced IT support vendor used by the Company. Our customer-facing operations, including our physical properties and our online and mobile gaming applications, have not been impacted by this incident and continue without disruption.
>
> After detecting the suspicious activity, we quickly activated our incident response protocols and implemented a series of containment and remediation measures to reinforce the security of our information technology network. We also launched an investigation, engaged leading cybersecurity firms to assist, and notified law enforcement and state gaming regulators. As a result of our investigation, on September 7, 2023, we determined that the unauthorized actor acquired a copy of, among other data, our loyalty program database, which includes driver's license

---

[13] See Zeba Siddiqui, *Hackers say they stole 6 terabytes of data from casino giants MGM, Caesars*, REUTERS (Sept. 14, 2023) https://www.reuters.com/business/casino-giant-caesars-confirms-data-breach-2023-09-14 (Last visited November 15, 2023).

[14] *Id.*

[15] See *SEC Form 8-K, Caesars Entertainment, Inc.*, CAESARS (Sept. 7, 2023) https://investor.caesars.com/static-files/0bc13ee5-34a9-402e-8e7a-824b9dba4e57 (last visited November 15, 2023)

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

> numbers and/or social security numbers for a significant number of members in the database. We are still investigating the extent of any additional personal or otherwise sensitive information contained in the files acquired by the unauthorized actor. We have no evidence to date that any member passwords/PINs, bank account information, or payment card information (PCI) were acquired by the unauthorized actor.

30. On or about September 7, 2023, Defendant posted a notice to the Caesars Informational Website concerning the breach ("Notice"). This Notice stated the following:

> **WHAT HAPPENED?**
>
> Caesars Entertainment ("Caesars") recently identified suspicious activity in its IT network resulting from a social engineering attack on an outside IT support vendor used by the Company.
>
> After detecting the suspicious activity at issue, we quickly activated our incident response protocols and implemented measures to reinforce the security of our network. We also launched an investigation, engaged leading cybersecurity firms to assist, and notified law enforcement and state gaming regulators.
>
> On September 7th, we determined that the unauthorized actor acquired, among other data, a copy of our loyalty program database, which includes driver's license numbers and/or Social Security numbers for a significant number of members in the database. We are still investigating if any additional personal or otherwise sensitive information was contained in the files acquired by the unauthorized actor.
>
> . . .
>
> **WHAT DATA WAS INVOLVED? / HOW WILL I KNOW IF MY DATA WAS INVOLVED?**
>
> The unauthorized actor acquired, among other data, a copy of our loyalty program database, which includes driver's license numbers and/or social security numbers for a significant number of members in the database. . . .

31. While Ceasars sought to minimize the damage caused by the breach, it cannot and has not denied that there was unauthorized access to the PII of Plaintiff and Class members.

32. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Caesars' Failure to Prevent, Identify and Timely Report the Data Breach.

33. Caesars admits that unauthorized third persons accessed from its network systems sensitive information about its current and former customers.

34. Caesars failed to take adequate measures to protect its computer and cloud storage systems against unauthorized access.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

35. Caesars was not only aware of the importance of protecting the PII that it maintains, as alleged, it promoted its capability to do so, as evident from Caesars Privacy Policies discussed supra paragraph 24. The PII that Caesars allowed to be exposed in the Data Breach is the type of private information that Caesar knew or should have known would be the target of cyberattacks.

36. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[16] Caesars failed to disclose that its systems and security practices were inadequate to reasonably safeguard their customer's sensitive personal information.

37. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach.[17] Immediate notification of a Data Breach is critical so that those impacted can take measures to protects themselves. Despite this guidance, Caesars delayed the notification of the Data Breach. As aforementioned, based on Caesars' disclosure to Maine's Attorney General's Office on October 6, 2023, the Data Breach is believed to have occurred on or around August 23, 2023. Yet, Caesars did not inform the public of the Data Breach until September 14, 2023, in an 8-K Filing with the SEC.

D. The Harm Caused by the Data Breach Now and Going Forward.

38. Victims of data breaches are susceptible to becoming victims of identity theft.

39. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[18]

---

[16] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited November 15, 2023).

[17] *Id.*

[18] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited November 15, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

40. The type of data that was accessed and compromised here – such as, full name and Social Security number – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

41. Plaintiffs and class members face a substantial risk of identity theft given that their Social Security numbers, addresses, dates of birth, and other important PII were compromised in the Data Breach. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

42. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

43. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[19]

44. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to reveal, PII about employees, customers and the public are housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[20]

---

[19] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited November 15, 2023).

[20] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR, April 3, 2018, *available at:* https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited November 15, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

45. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

46. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

47. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[24]

48. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[25]

---

[21] *Id.*

[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited November 15, 2023).

[23] *Id.*

[24] *Experts advise compliance not same as security*, RELIAS MEDIA https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (Last visited November 15, 2023).

[25] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

49. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[26] Defendant did not rapidly report to Plaintiffs and Class members that their PII had been stolen.

50. As a result of the Data Breach, the PII of Plaintiffs and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their PII against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

51. In addition to a remedy for economic harm, Plaintiffs and Class members maintain an interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

52. Defendant disregarded the rights of Plaintiffs and Class members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to

---

021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (Last visited November 15, 2023).

[26] *Id.*

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

adequately safeguard Plaintiffs' and Class members' PII; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

53. The actual and adverse effects to Plaintiffs and Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiffs and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiffs and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ACTION ALLEGATIONS

54. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the data breach publicly announced by Caesars in September 2023 (the "Class").

55. Plaintiff also seeks certification of a New Jersey Subclass, defined as follows:

> All New Jersey residents whose personal information was compromised in the data breach publicly announced by Caesars in September of 2023 (the "New Jersey Subclass").

56. Plaintiff also seeks certification of a New York Subclass, defined as follows:

> All New York residents whose personal information was compromised in the data breach publicly announced by Caesars in September of 2023 (the "New York Subclass").

57. Plaintiff also seeks certification of a Maryland Subclass, defined as follows:

> All Maryland residents whose personal information was compromised in the data breach publicly announced by Caesars in September of 2023 (the "Maryland

STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

Subclass").

58. Plaintiff also seeks certification of a California Subclass, defined as follows:

> All California residents whose personal information was compromised in the data breach publicly announced by Caesars in September of 2023 (the "California Subclass").

59. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

60. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

61. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

62. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, Plaintiffs estimate that the Class is comprised of millions of Class members. The Class is sufficiently numerous to warrant certification.

63. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of other Class Members because they all had their PII compromised as a result of the Data Breach. Plaintiffs are members of the Class and their claims are typical of the claims of the members of the Class. The harm suffered by Plaintiffs is similar to that suffered by all other Class members that was caused by the same misconduct by Defendant.

64. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

65. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

66. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class members present common questions of law or fact, which predominate over any questions affecting only individual Class members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's storage of Class Member's PII was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiffs' and Class Members' PII;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiffs' and Class Members' privacy;

g. Whether Defendant's conduct violated the statutes as set forth herein;

h. Whether Defendant took sufficient steps to secure its customers' PII;

i. Whether Defendant was unjustly enriched;

j. The nature of relief, including damages and equitable relief, to which Plaintiffs and members of the Class are entitled.

67. Information concerning Defendant's policies is available from Defendant's records.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

68. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

69. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

70. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

71. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

72. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

73. Plaintiffs bring this claim individually and on behalf of the Class members.

74. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

75. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII.

76. Defendant had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' PII within its possession was compromised and precisely the type(s) of information that were compromised.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

77. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its customers' PII.

78. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

79. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

80. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII.

81. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

82. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII within Defendant's possession.

83. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' PII.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

84. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

85. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Member's PII. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the personal customer information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their networks' vulnerabilities; and failed to implement policies to correct security issues.

86. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

87. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs and Class Members' PII would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

88. It was foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII would result in injuries to Plaintiffs and Class Members.

89. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII to be compromised.

90. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.

91. As a result of Defendant's failure to timely notify Plaintiffs and Class Members that their PII had been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

92. As a result of Defendant's negligence and breach of duties, Plaintiffs and Class

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiffs and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

93. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

94. Plaintiffs and the Class provided and entrusted their PII to Defendant. Plaintiffs and the Class provided their PII to Defendant, either directly or indirectly through Defendant's clients, as part of Defendant's regular business practices.

95. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class members in its possession was secure.

96. Pursuant to these implied contracts, Plaintiffs and Class members provided Defendant with their PII in order for Defendant to provide services, for which Defendant is compensated. In exchange, Defendant agreed to, among other things, and Plaintiffs understood that Defendant would: (1) provide services to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and (3)

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

protect Plaintiffs' and Class members PII in compliance with federal and state laws and regulations and industry standards.

97. Implied in these exchanges was a promise by Defendant to ensure the PII of Plaintiffs and Class members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiffs' and Class members' PII.

98. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiffs' and Class members' PII to be accessed in the Data Breach.

99. Indeed, implicit in the agreement between Defendant and its customers was the obligation that both parties would maintain information confidentially and securely.

100. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiffs and Class members would provide their PII in exchange for services by Defendant. These agreements were made by Plaintiffs and Class members as Defendant's customers.

101. When the parties entered into an agreement, mutual assent occurred. Plaintiffs and Class members would not have disclosed their PII to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiffs' and Class members' PII if it did not intend to provide Plaintiffs and Class members with its services.

102. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure and/or use.

103. Plaintiffs and Class Members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

104. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

105. Defendant breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII.

106. Defendant's failure to implement adequate measures to protect the PII of Plaintiffs and Class Members violated the purpose of the agreement between the parties.

107. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class Members' PII, which Plaintiffs and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiffs and Class members.

108. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiffs and Class Members, Plaintiffs and the Class Members suffered damages as described in detail above.

COUNT III
VIOLATION OF THE MARYLAND CONSUMER PROTECTION ACT
MD CODE COMMERCIAL LAW, § 13-301, *et seq.*
(On Behalf of Plaintiff and the Maryland Subclass)

109. Plaintiff re-alleges and incorporates each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

110. Maryland Class Members are "consumers" under the Md. Code Ann., Com. Law § 13-101.

111. Caesars provides services that are "consumer goods" and/or "consumer services" under the Md. Code Ann., Com. Law § 13-101.

112. Defendant operates in Maryland, and in doing so engages in unlawful trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of its services in violation of Md. Code Ann., Com. Law § 13-301, including but not limited to the following: a) Defendant misrepresented material facts, pertaining to the sale of its services, to the Maryland Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Maryland Class Members' PII from unauthorized disclosure, release, data breaches, and theft in violation of Md. Code Ann.,

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi) which state:

a. Defendant misrepresented material facts, pertaining to the sale of its services, to the Maryland Class by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Maryland Class Members' PII in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);

b. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for the Maryland Class Members' PII in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);

c. Defendant engaged in unfair acts and practices with respect to the sale of its services by failing to maintain the privacy and security of Maryland Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45); Maryland's Privacy of Consumer Financial and Health Information regulations (Md. Code Regs. 31.16.08.01, et seq.); Maryland's data breach statute (Md. Code Ann. Com. Law § 14-3503), and Maryland's Social Security Number Privacy Act (Md. Code Ann., Com. Law § 14-3401, et seq.);

d. Defendant engaged in unfair acts and practices with respect to the sale of its services by failing to disclose the Data Breach to Maryland Class Members in a timely and accurate manner, in violation of Md. Code Com. Law § 14-3504(b)(3);

e. Defendant engaged in unfair acts and practices with respect to the sale of its services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Maryland Class Members' PII from further unauthorized disclosure, release, data breaches, and theft.

113. As a result of Defendant's deceptive acts and practices, Plaintiffs suffered substantial

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

injury that they could not reasonably avoid.

114. Defendant knew or should have known that its systems and security practices were inadequate to safeguard Maryland Class Members' PII and that risk of a data breach or theft was highly likely. Defendant's unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Maryland Class.

115. As a direct and proximate result of Defendant's unlawful practices, Maryland Class Members suffered injury and/or damages.

116. Maryland Class Members seek relief under Md. Code Ann., Com. Law § 13-408, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs.

COUNT IV
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and California Subclass Members)

117. Plaintiff re-alleges and incorporates each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

118. Plaintiff and the California Subclass bring this claim on behalf of the California Subclass against Defendant.

119. Defendant has engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code Sections 17200, et seq.

120. Defendant stored the PII of Plaintiff and Subclass Members in its computer systems.

121. Defendant knew or should have known that it did not maintain reasonable and appropriate security measures that complied with federal regulations to safeguard consumers' PII. As evident from the Data Breach, Defendant failed to properly vet the data security of its third-party agents and vendors to whom it provided sensitive customer PII.

122. Moreover, Defendant failed to disclose that Plaintiffs' and Subclass Members' PII were susceptible to hackers as a result of Defendant's inadequate data security measures, and that

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Defendant was the only one in possession of that material information. Defendant had a duty to disclose information regarding the susceptibility of Plaintiffs' and Subclass Members' PII.

123. Defendant's actions and inactions violated the "unlawful" prong of the UCL. Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety and security of their computer systems, and its ability to safely store Plaintiff's and Subclass Members' PII.

124. Defendant further violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards in its data security practices, by failing to ensure its affiliates with which it directly or indirectly shared the PII did the same, and by failing to timely notify Plaintiff and Class Members of the Data Breach.

125. Had Defendant complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiff and Class Members of the Data Breach.

126. Defendant's actions and inactions further violated the "unfair" prong of the UCL.

127. Under the "balancing test," Defendant engaged in unfair business practices. The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweighs any perceived utility. Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendant's data security cannot be said to have had any utility at all. All of Defendant's actions and omissions in this respect were clearly injurious to Plaintiff and Subclass Members, directly causing the harms alleged below.

128. Similarly, Defendant engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described herein, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the California law.

129. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects thousands of Subclass Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Subclass Members' PII to third parties without their consent, diminution in value of their PII.

130. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Subclass Members. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiffs and Subclass Members outweighed their utility, if any. Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively declared public policy, and is immoral, unethical, oppressive, and unscrupulous.

131. Plaintiff and Subclass Members continue to suffer harm, as Plaintiff's and Subclass Members' PII remains in Defendant's possession, without adequate protection, and remains in the hands of those who obtained it without their consent.

132. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); see also, e.g., *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

133. Plaintiff and Class Members suffered injury in fact and lost money or property as a result of Defendant's violations of the UCL. Plaintiffs and the California Class suffered from entering into transactions with Defendant that should have included adequate data security for their

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

PII, by experiencing a diminution of value in their Private Information as a result if its theft by cybercriminals, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their PII, the right to control that information, and additional losses as described above.

134. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT V
VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT
N.J.S.A. 56:8-1
(On Behalf of Plaintiff and the New Jersey Subclass)

141. Plaintiff incorporates the above factual allegations as if fully set forth herein.

142. Plaintiff and all Class Members are "consumers" as defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1.

143. Defendant is a "person" as defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

144. Defendant's conduct as alleged here related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

145. Defendant engaged in the advertisement, offer, or sale of goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of New Jersey.

146. Defendant directly solicited Plaintiff and Class Members to do business and uniformly and knowingly misrepresented that by opening a loyalty rewards account with Caesars, their PII was safe, confidential, and protected from intrusion, hacking, or theft.

147. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiff and Class Members' PII by implementing and maintaining reasonable security measures.

148. Defendant intended to mislead Plaintiff and Class Members and to induce them to rely on the various misrepresentations and omissions they made.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

149. Defendant failed to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' PII in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

150. Defendant failed to provide notice to Plaintiff and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

151. Defendant's acts and omissions, as set forth here, indicate a lack of good faith, honesty in fact and observance of fair dealing, to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

152. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class Members are required to expend sums to protect and recover their PII, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII, and thereby suffered ascertainable economic loss.

153. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT VI
VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law §§ 349, et seq.
(On Behalf of Plaintiff and the New York Subclass)

154. Plaintiffs incorporate the above factual allegations as if fully set forth herein.

155. Defendant engaged in deceptive acts or practices in the conducting of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to maintain adequate security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

156. Defendant's false representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Caesars' data security and ability to protect the confidentiality of consumers' PII.

157. Defendant acted intentionally, knowingly, and maliciously in violating New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass Members' rights in their privacy. Defendant's past data breaches put it on notice that its security and privacy protections were inadequate.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

158. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, measurable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Caesars' services; loss of the value of access to their PII; and the value of identity protection services made necessary through the disclosure of their PII by the Data Breach.

159. As described above, the deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and New York Subclass Members that they could not have reasonably avoided.

160. Furthermore, Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

161. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

COUNT VII
UNJUST ENRICHMENT
(On behalf of Plaintiffs and All Class Members)

162. Plaintiffs incorporate the above factual allegations as if fully set forth herein.

163. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

164. Plaintiffs and Class Members conferred a benefit upon Defendant by using Defendant's services.

165. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiffs' PII, as this was used for Defendant administer its services to Plaintiffs and the Class.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

166. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' services and their PII because Defendant failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII to Defendant or utilized its services had they known Defendant would not adequately protect their PII.

167. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representative of the Class and his counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: November 20, 2023

Respectfully submitted,

/s/ Nathan R. Ring

Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

Mark S. Reich*
Courtney E. Maccarone*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
4th Floor, Suite #427
New York, NY 10006
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: cmaccarone@zlk.com

Counsel for Plaintiff and the Putative Class

**pro hac vice* forthcoming